Web Application Security Testing Report

# Brute Force Attack Using Burp Suite Intruder

This report details the process and findings of performing a brute force attack on the sample web application’s login functionality using Burp Suite Intruder. The goal was to identify valid user credentials and evaluate the application's resilience to authentication attacks.

## Testing Environment and Tools

• **Testing platform**: DVWA running on Kali Linux VM  
• **Tool used**: Burp Suite Intruder  
• **Target URL:** http://localhost:8080/vulnerabilities/brute/

## Test Procedure

1. Configured Burp Suite proxy and set Firefox browser proxy to intercept traffic.  
2. Navigated to the login page of the target application and attempted to log in with test credentials.  
3. Intercepted the login POST request and sent it to Burp Intruder.  
4. Cleared default payload positions and manually set fuzz positions for the username and password parameters.  
5. Created two payload sets: a list of usernames and a list of passwords.  
6. Started the Intruder attack using the Cluster Bomb attack type to test all combinations.  
7. Monitored response statuses and headers for indications of successful login.

## Findings

• Most login attempts redirected back to the login page, indicated by HTTP response header:  
 **Location: login.php**  
• Successful login attempts redirected to the application’s main page, indicated by:  
 **Location: index.php**  
• The difference in redirect location allowed clear identification of valid username-password pairs.  
• This method reliably distinguished between failed and successful authentication attempts.

## Recommendations

• Implement account lockout or throttling mechanisms after several failed login attempts to mitigate brute force attacks.  
• Use multi-factor authentication (MFA) to add an additional layer of security.  
• Monitor and log authentication attempts to detect suspicious activity.  
• Employ CAPTCHAs on login forms to reduce automated attacks.  
• Ensure secure password policies and educate users on creating strong passwords.

## Conclusion

The brute force testing confirmed that the application does not have protections against rapid repeated login attempts, making it vulnerable to credential stuffing and brute force attacks. Implementing the recommended security measures will improve the application's resilience against such threats.